DOCUMENT RESUME

ED 282 520 IR 012 663

TITLE	The Computer Fraud and Abuse Act of 1986. Hearing before the Committee on the Judiciary, United States Senate, Ninety-Ninth Congress, Second Session on S.2281, a Bill To Amend Title 18, United States Code, To Provide Additional Penalties for Fraud and Related Activities in Connection with Access Devices and Computers, and for Other Purposes.
INSTITUTION	Congress of the U.S., Washington, D.C. Senate Committee on the Judiciary.
REPORT NO	Senate-Hrg-99-863
PUB DATE	16 Apr 86
NOTE	52p.; Serial No. J-99-96. Document contains small, broken type.
AVAILABLE FROM	Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402.
PUB TYPE	Legal/Legislative/Regulatory Materials (090)
EDRS PRICE	MF01/PC03 Plus Postage.
DESCRIPTORS	*Access to Information; *Computers; *Crime; Disclosure; *Federal Legislation; Fines (Penalties); Hearings; Privacy
IDENTIFIERS	Computer Security; Congress 99th; Information Value

ABSTRACT

The proposed legislation--S. 2281--would amend federal laws to provide additional penalties for fraud and related activities in connection with access devices and computers. The complete text of the bill and proceedings of the hearing are included in this report. Statements and materials submitted by the following committee members and witnesses are provided: (1) Senator Paul Simon; (2) Senator Strom Thurmond, Chairman; (3) Senator Jeremiah Denton; (4) Senator Paul S. Trible; (5) Victoria Toensing, Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice; (6) Joseph Tompkins, attorney, Sidley & Austin, Washington, D.C.; and (7) John J. Sponski, group executive officer, Sovran Financial Corporation, Richmond, Virginia. (MES)

IR

S. HRG. 99-863

THE COMPUTER FRAUD AND ABUSE ACT OF 1986

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY UNITED STATES SENATE

NINETY-NINTH CONGRESS

SECOND SESSION

ON

S. 2281

A BILL TO AMEND TITLE 18, UNITED STATES CODE, TO PROVIDE ADDITIONAL PENALTIES FOR FRAUD AND RELATED ACTIVITIES IN CONNECTION WITH ACCESS DEVICES AND COMPUTERS, AND FOR OTHER PURPOSES

APRIL 16, 1986

Serial No. J-99-96

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
62-543 O WASHINGTON : 1986

For sale by the Superintendent of Documents, Congressional Sales Office
U.S. Government Printing Office, Washington, DC 20402

COMMITTEE ON THE JUDICIARY

STROM THURMOND, South Carolina, *Chairman*

CHARLES McC. MATHIAS, JR., Maryland	JOSEPH R. BIDEN, JR., Delaware
PAUL LAXALT, Nevada	EDWARD M. KENNEDY, Massachusetts
ORRIN G. HATCH, Utah	ROBERT C. BYRD, West Virginia
ALAN K. SIMPSON, Wyoming	HOWARD M. METZENBAUM, Ohio
JOHN P. EAST, North Carolina	DENNIS DECONCINI, Arizona
CHARLES E. GRASSLEY, Iowa	PATRICK J. LEAHY, Vermont
JEREMIAH DENTON, Alabama	HOWELL HEFLIN, Alabama
ARLEN SPECTER, Pennsylvania	PAUL SIMON, Illinois
MITCH McCONNELL, Kentucky	

DENNIS W. SHEDD, *Chief Counsel and Staff Director*
DIANA L. WATERMAN, *General Counsel*
MELINDA KOUTSOUMPAS, *Chief Clerk*
MARK H. GITENSTEIN, *Minority Chief Counsel*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

PROPOSED LEGISLATION

CHRONOLOGICAL LIST OF WITNESSES

ALPHABETICAL LISTING AND MATERIALS SUBMITTED

THE COMPUTER FRAUD AND ABUSE ACT OF 1986—S. 2281

WEDNESDAY, APRIL 16, 1986

U.S. SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The committee met, pursuant to notice, at 9:48 a.m., in room SD-628, Dirksen Senate Office Building, Hon. Paul Laxalt presiding.

Also present: Senator Simon.

Staff present: William S. Miller, Jr., majority counsel; and Terry Wooten, majority counsel.

OPENING STATEMENT OF SENATOR PAUL SIMON

Senator SIMON. The hearing will come to order.

I am temporarily pinch-hitting until the committee chair is here. I am interested in the subject. I do not claim to have any expertise. I am here to learn, and hope our witnesses will provide that opportunity.

The first witness is Senator Paul Trible, the chief sponsor of the legislation, and we are very pleased to have our colleague here on what is a very important question.

STATEMENT OF HON. PAUL S. TRIBLE, A U.S. SENATOR FROM THE STATE OF VIRGINIA

Senator TRIBLE. Senator Simon, I thank you for your warm welcome and I would ask at this time that my full statement be made a part of the record.

Senator SIMON. It will be.

Senator TRIBLE. I will summarize that statement at this time, with your permission.

Senator SIMON. You have my full permission to do that.

Senator TRIBLE. Mr. Chairman, I appreciate the opportunity to testify today on S. 2281, a bill that I have sponsored, along with Senator Laxalt and others, to combat the growing problem of computer crime.

I would say to my friend from Illinois that among the many cosponsors is Senator Dixon, your colleague from Illinois. So I hope that you, too, will take a look at this measure and perhaps cosponsor this effort.

For the past two decades, the United States has experienced a technological revolution. Widespread computer use has brought a great many benefits to American business and to all of our lives.

But it has also created a new type of criminal, one that uses computers to steal, to defraud, and to abuse the property of others.

A recent survey by the American Bar Association found that almost one-half of those companies and government agencies that responded had been victimized by some form of computer crime. The known financial loss from these crimes was estimated as high as $730 million, and the report concluded that computer crime is among the worst white-collar offenses.

In addition, pirate bulletin boards have sprung up around the country for the sole purpose of exchanging passwords to other people's computer systems. In Virginia alone, three such bulletin boards carry information on how to break into computers belonging to the Defense Department, the Republican National Committee, and other groups.

Senator Simon, it is time to dispel the notion that computer crime is not a serious offense. To that end, I introduced legislation early in 1985 to strengthen Federal penalties for computer-related crimes. That bill, S. 440, was the subject of hearings before Senator Laxalt's Subcommittee on Criminal Law last October.

In the months since, I have worked closely with that chairman, Senator Laxalt, and with Congressman Hughes of New Jersey, who heads up the appropriate subcommittee in the House of Representatives, and I believe we have reached a consensus on the proper scope of Federal jurisdiction over computer crime. This measure before us, S. 2281, embodies that consensus.

This legislation will assert Federal jurisdiction only in those cases in which there is a compelling Federal interest. It will broaden protections currently given computers belonging to the Federal Government. It will afford similar protections to computers belonging to federally insured financial institutions, and it will proscribe certain computer crimes that are interstate in character.

In more specific terms, my proposal will modify slightly the existing computer crime statute in order to clarify its intent. For example, the Justice Department has expressed concerns about whether present law covers acts of simple trespass on Government computers or whether it requires a further showing that the data was used or modified.

S. 2281 will make it clear that the present subsection (a)(3) is a trespass offense. In addition, my bill will delete entirely the provision in the present computer crime law relating to conspiracies. A conspiracy to commit a computer crime will be covered instead by the general Federal conspiracy statute, 18 U.S.C. 371.

S. 2281 will also broaden the protections presently given data relating to individuals' credit histories to include computerized records of all customers, individual and corporate, of federally insured financial institutions.

Now, in addition, this legislation will create several new computer crime offenses, and let me enumerate those very briefly.

The new section (a)(4) will penalize thefts of property via computer that are committed with an intent to defraud. It will require a showing that the use of the computer was integral to the intended fraud and was not merely incidental.

The bill will also proscribe intentional destruction of computerized property belonging to another. Such an act may include out-

right deletion of information or substantial damage to it. It may also include an act intended to alter another's computer password, thereby denying them access to their own data.

In either case, this legislation will ensure that destruction of computerized data is punished as surely as we now punish abuses in more traditional forms of property.

Now, both the theft and the destruction of property will be covered by this bill when they are committed against computers belonging to the Federal Government or to federally insured financial institutions. Moreover, the same offenses will be covered when the computers involved are located in two or more different States.

Finally, this bill will permit prosecution of those individuals who, possessing a clear intent to defraud, traffic in computer passwords belonging to others. As I have mentioned, several pirate bulletin boards are operating in my home State of Virginia which now carry information on how to break into computers belonging to others. This legislation will provide misdemeanor penalties for such a crime.

Mr. Chairman, there remains a vast array of computerized data that is wholly unprotected against acts of theft, vandalism and trespass. In the Government's race to protect this computer data against crime, the hour is late. Quite simply, the criminals have the technological edge.

I believe this Congress must act quickly and give Federal prosecutors the tools to respond to computer-related crimes. Over the past several months, as I have said, I have worked closely with Senator Laxalt; Congressman Hughes, the Chairman of the House Subcommittee on Crime; and several other of our colleagues here in the Senate to fashion a computer crime statute that is properly focused.

I believe this measure strikes a proper balance between the clear interests of the Federal Government in computer crime and the ability of the States to investigate and prosecute such offenses.

I hope the committee will agree, and I hope the committee, with your support and leadership, will move quickly to approve Senate bill 2281.

Senator SIMON. I thank you for what appears to be both a good and a needed bill.

Let me ask you one question here, and I am a nontechnical, noncomputer person. When you talk about simple trespass and making that a crime, can simple trespass be accidental?

Senator TRIBLE. Well, frequently, an offender who has accessed a Government computer without proper authorization will not steal or damage the computer data. But, nevertheless, the offender is treading where he ought not to be, and he should be subject to prosecution in appropriate cases, just as surely as someone who walks on to, let us say, a sensitive Government property without proper authorization.

So it is my view that there ought to be a law saying that such simple trespass is indeed unlawful. But, yes, the answer to your question is the simple trespass would be subject to prosecution. But, obviously, it would only be subject to prosecution in those cases where it was a serious offense.

Senator SIMON. Is simple trespass something that can happen accidentally or must it be intentional?

Senator TRIBLE. Well, the whole body of this legislation, the whole thrust is to go the extra mile to ensure that a contemplated criminal conduct is intentional; that it is unlawful in character.

Senator SIMON. We thank you very much. If you would care to join us here—in fact, since I have to be at another meeting in a few minutes——

Senator TRIBLE. Well, I chaired at least part of the last hearing that focused on computer crime. I feel like an honorary member of this committee. I must confess, though, I have got to go mark up a bill in the Foreign Relations, so I guess——

Senator SIMON. You are not going to be able——

Senator TRIBLE. I cannot stay, as much as I would like.

Senator SIMON. OK, all right.

Senator TRIBLE. I would like to be here to hear the Department of Justice speak in favor of this legislation, but I think I will have to read Victoria's statement instead.

Senator SIMON. That is an assumption on your part, Senator Trible. All right.

Senator TRIBLE. Thank you, sir.

Senator SIMON. Thank you.

[The prepared statements of Senators Trible and Thurmond and the text of S. 2281 follow:]

PREPARED STATEMENT OF SENATOR PAUL S. TRIBLE

Mr. Chairman, I appreciate the opportunity to testify today on S. 2281, a bill I have sponsored, together with Senator Laxalt and others, to combat the growing problem of computer crime.

For the past two decades, the United States has experienced a technological revolution. Widespread computer use has brought a great many benefits to American business and Americans' lives. But it has also created a new type of criminal—one who uses computers to steal, to defraud, and to abuse the property of others.

A recent survey by the American Bar Association found that almost one-half of those companies and Government agencies that responded had been victimized by some form of computer crime. The known financial loss from those crimes was estimated as high as $730 million, and the report concluded that computer crime is among the worst white-collar offenses.

In addition, pirate bulletin boards have sprung up around the country for the sole purpose of exchanging passwords to other people's computer systems. In Virginia alone, three such bulletin boards carry information on how to break into computers belonging to the Defense Department and the Republican National Committee.

Mr. Chairman, it is time to dispel the notion that computer crime is not a serious offense. The fact is, the computer criminal is a lawbreaker just like any other, and he deserves to be treated as such.

To that end, I introduced legislation early in 1985 to strengthen Federal penalties for computer-related crime. That bill, S. 440, was the subject of hearings before the Senate Subcommittee on Criminal Law last October. In the months since, I have worked closely with the Chairman of that subcommittee to reach a consensus on the proper scope of Federal jurisdiction over computer crime. I believe S. 2281 embodies that consensus.

This legislation will assert Federal jurisdiction only in those cases in which there is a compelling Federal interest. Accordingly, S. 2281 will broaden the protections currently given computers belonging to the Federal Government. It will afford similar protections to computers belonging to federally insured financial institutions. And it will proscribe certain computer crimes that are interstate in nature.

AMENDMENTS TO PRESENT LAW

In more specific terms, Mr. Chairman, my proposal will modify slightly the existing computer crime statute (18 U.S.C. 1030) in order to clarify its intent.

For example, the Justice Department has expressed concerns about whether present law covers acts of simple trespass on Government computers, or whether it requires a further showing that the data was used or modified. S. 2281 will make clear that present subsection (a)(3) is a trespass offense. Frequently, an offender who has accessed a Government computer without proper authorization will not steal or damage the computer data. Nevertheless, the offender in such cases is treading where he ought not to be, and he should be subject to prosecution just as surely as someone who walks onto sensitive Government property without proper authorization.

In addition, my bill will delete entirely the provision of the present computer crime law relating to conspiracies. A conspiracy to commit a computer crime will be covered instead by the general conspiracy statute (18 U.S.C. 371).

S. 2281 will also broaden the protections presently given data relating to individuals' credit histories. It is an offense under existing law to steal computerized information on individuals' relationships with consumer reporting agencies. The premise of that offense is to protect the privacy of customers of such agencies. My bill will broaden those privacy protections to include computerized records of all customers—individual and corporate—of federally insured financial institutions.

NEW OFFENSES

In addition, Mr. Chairman, this legislation will create several new computer crime offenses.

The new subsection (a)(4) will penalize thefts of property via computer that are committed with an intent to defraud. It will require a showing that the use of the computer was integral to the intended fraud, and was not merely incidental. An individual possessing an intent to defraud should not be punished for merely storing information in a computer, any more than he should be punished for storing that information in a file cabinet or card file. The use of a computer by one who has devised a scheme to defraud should constitute an offense only when the computer was used to obtain property of another which furthers the intended fraud.

This bill will also proscribe intentional destruction of computerized property belonging to another. Such an act may include outright deletion of information, or substantial damage to it. It may also include an act intended to alter another's computer password, thereby denying him access to his own data. In either case, S. 2281 will ensure that destruction of computerized data is punished as surely as we now punish abuses of more traditional forms of property.

Both the theft and the destruction of property will be covered by this bill when they are committed against computers belonging to the Federal Government or federally insured financial institutions. The same offenses will be covered when the computers involved are located in two or more different States.

Finally, this bill will permit prosecution of those individuals who, possessing a clear intent to defraud, traffic in computer passwords belonging to others. As I have mentioned, several pirate bulletin boards are operating in my home State of Virginia which carry information on how to break into computers belonging to others. S. 2281 will provide misdemeanor penalties for such a crime.

Mr. Chairman, there remains a vast array of computerized data that is wholly unprotected against acts of theft, vandalism, and trespass. In the Government's race to protect this computer data against crime, the hour is late. Quite simply, the criminals have the technological edge.

I believe this Congress must act quickly, and give Federal prosecutors the tools to respond to computer-related crimes. Over the past several months, I have worked closely with Senator Laxalt and Congressman Hughes, the chairman of the House Subcommittee on Crime, to fashion a computer crime statute that is narrowly focused. I believe this measure strikes a proper balance between the clear interests of the Federal Government in computer crime, and the ability of the States to investigate and prosecute such offenses. I hope that this committee will agree, and will move quickly to approve S. 2281.

I look forward to working with the committee in the days ahead, and I will be happy to answer any questions at this time.

PREPARED STATEMENT OF CHAIRMAN STROM THURMOND

Good Morning. Today we are here to examine legislation that will provide additional penalties for fraud and related activities in connection with computers and access devices.

This proposed legislation has a two-fold objective. First, it is designed to make necessary adjustments to title 18, section 1030, of the United States Code to allow for more effective punishment of individuals who commit computer crime. Second, this legislation will add new computer crime offenses to section 1030 not contemplated in the original legislation. This compelling expansion of section 1030 offenses will act to protect those private entities who store confidential information on computers not subject to public disclosure. As well, the expansion of prosecutable offenses will protect the United States Government as well as private entities from suspecting individuals who access computers to commit fraud and to alter or destroy stored data that could not be replaced.

I welcome a panel of distinguished witnesses from organizations who rely on computers in their day to day business operations. I am confident that today's witnesses will provide invaluable insight into this proposed legislation that will enhance and improve the present Federal legislation.

II

99TH CONGRESS
2D SESSION

S. 2281

To amend title 18, United States Code, to provide additional penalties for fraud and related activities in connection with access devices and computers, and for other purposes.

IN THE SENATE OF THE UNITED STATES

APRIL 10 (legislative day, APRIL 8), 1986

Mr. TRIBLE (for himself, Mr. LAXALT, Mr. DENTON, Mr. ARMSTRONG, and Mr. DIXON) introduced the following bill; which was read twice and referred to the Committee on the Judiciary

---

A BILL

To amend title 18, United States Code, to provide additional penalties for fraud and related activities in connection with access devices and computers, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Computer Fraud and Abuse Act of 1986".

SEC. 2. SECTION 1030 AMENDMENTS.

(a) MODIFICATION OF DEFINITION OF FINANCIAL INSTITUTION.—Section 1030(a)(2) of title 18, United States Code, is amended—

(1) by striking out "knowingly" and inserting "intentionally" in lieu thereof; and

(2) by striking out "as such terms are defined in the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.),".

(b) MODIFICATION OF EXISTING GOVERNMENT COMPUTERS OFFENSE.—Section 1030(a)(3) of title 18, United States Code, is amended—

(1) by striking out "knowingly" and inserting "intentionally" in lieu thereof;

(2) by striking out ", or having accessed" and all that follows through "prevents authorized use of, such computer";

(3) by striking out "It is not an offense" and all that follows through "use of the computer."; and

(4) by striking out "if such computer is operated for or on behalf of the Government of the United States and such conduct affects such operation" and inserting in lieu thereof "if such computer is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, if such computer is used by or for the Government of the United States and such conduct affects such use".

(c) MODIFICATION OF AUTHORIZED ACCESS ASPECT OF OFFENSES.—Paragraphs (1) and (2) of section 1030(a) of title 18, United States Code, are each amended by striking out ", or having accessed" and all that follows through "does not extend" and inserting "or exceeds authorized access" in lieu thereof.

(d) NEW OFFENSES.—Section 1030(a) of title 18, United States Code, is amended by inserting after paragraph (3) the following:

"(4) knowingly and with intent to defraud, accesses a Federal interest computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer;

"(5) intentionally accesses a Federal interest computer without authorization, and by means of one or more instances of such conduct alters information in that computer, or prevents authorized use of that computer, and thereby causes loss to another of a value aggregating $1,000 or more during any one year period; or

"(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar

information through which a computer may be accessed without authorization, if—

"(A) such trafficking affects interstate or foreign commerce; or

"(B) such computer is used by or for the Government of the United States;".

(e) ELIMINATION OF SECTION SPECIFIC CONSPIRACY OFFENSE.—Section 1030(b) of title 18, United States Code, is amended—

(1) by striking out "(1)"; and

(2) by striking out paragraph (2).

(f) PENALTY AMENDMENTS.—Section 1030 of title 18, United States Code, is amended—

(1) by striking out "of not more than the greater of $10,000" and all that follows through "obtained by the offense" in subsection (c)(1)(A) and inserting "under this title" in lieu thereof;

(2) by striking out "of not more than the greater of $100,000" and all that follows through "obtained by the offense" in subsection (c)(1)(B) and inserting "under this title" in lieu thereof;

(3) by striking out "or (a)(3)" each place it appears in subsection (c)(2) and inserting ", (a)(3) or (a)(6)" in lieu thereof;

(4) by striking out "of not more than the greater of $5,000" and all that follows through "created by the offense" in subsection (c)(2)(A) and inserting "under this title" in lieu thereof;

(5) by striking out "of not more than the greater of $10,000" and all that follows through "created by the offense" in subsection (c)(2)(B) and inserting "under this title" in lieu thereof;

(6) by striking out "not than" in subsection (c)(2)(B) and inserting "not more than" in lieu thereof;

(7) by striking out the period at the end of subsection (c)(2)(B) and inserting "; and" in lieu thereof; and

(8) by adding at the end of subsection (c) the following:

"(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(5) of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

"(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4) or (a)(5) of this section which occurs after a conviction for another offense

under such subsection, or an attempt to commit an offense punishable under this subparagraph.".

(g) CONFORMING AMENDMENTS TO DEFINITIONS PROVISION.—Section 1030(e) of title 18, United States Code, is amended—

(1) by striking out the comma after "As used in this section" and inserting a one-em dash in lieu thereof;

(2) by aligning the remaining portion of the subsection so that it is cut in two ems and begins as an indented paragraph, and inserting "(1)" before "the term";

(3) by striking out the period at the end and inserting a semicolon in lieu thereof; and

(4) by adding at the end thereof the following:

'(2) the term 'Federal interest computer' means a computer—

"(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects such use; or

"(B) which is one of two or more computers used in committing the offense, not all of which are located in the same State;

"(3) the term 'State' includes the District of Columbia, the Commonwealth of Puerto Rico, and any other possession or territory of the United States;

"(4) the term 'financial institution' means—

"(A) a bank with deposits insured by the Federal Deposit Insurance Corporation;

"(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

"(C) an institution with accounts insured by the Federal Savings and Loan Insurance Corporation;

"(D) a credit union with accounts insured by the National Credit Union Administration;

"(E) a member of the Federal home loan bank system and any home loan bank; and

"(F) any institution of the Farm Credit System under the Farm Credit Act of 1971;

"(5) the term 'financial record' means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution; and

62-543 0 - 86 - 2

"(6) the term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.".

(h) LAW ENFORCEMENT AND INTELLIGENCE ACTIVITY EXCEPTION.—Section 1030 of title 18, United States Code, is amended by adding at the end the following new subsection:

"(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.".

O

Senator SIMON. Victoria Toensing, if I am pronouncing it correctly, the Deputy Assistant Attorney General.

STATEMENT OF VICTORIA TOENSING, DEPUTY ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, U.S. DEPARTMENT OF JUSTICE

Ms. TOENSING. Good morning.

Senator SIMON. Thank you very much. We welcome you.

Ms. TOENSING. Good morning, Mr. Chairman. I have a much longer complete statement that I would like to submit for the record.

Senator SIMON. It will be in the record.

Ms. TOENSING. And I promise to make my own remarks shorter. I also had to promise Senator Trible that I would be positive in my statements, Mr. Chairman, so I am going to do the best that I can.

I testified before this committee last fall and explained the problems that the Justice Department had on the present computer crime act; we were really having a great deal of problems with it.

At that time, I promoted the administration's computer crime bill. I would like to commend the subcommittee and, in particular, Senators Trible and Laxalt for all the work that they have done. I worked on Senate staff myself for 3 years, so I know all the work that the staff has also done on this project.

The present bill is much improved for us in addressing the problem of computer crime. What I would like to do is put on the record that we are basically supporting S. 2281. We are still looking at it with some hope for getting a few more changes in it that we think will make it easier for us to prosecute.

Let me outline for you the four main principles that we would like to see in a computer crime bill. Before I do that, I would like to explain that when I use the shorthand term of "Federal computer," what I really mean is that it is a computer owned or operated on behalf of the United States or of a federally insured financial institution. But I will use the shorthand of just a "Federal computer" so we all know what we are talking about.

The first principle that we would like to see is that it be a crime to have unauthorized access to any kind of Federal computer without the obtaining of any information. It is simply that there should not be any unauthorized access.

No. 2, that there be a computer fraud offense that is patterned after our present fraud statutes, and that this apply to both the Federal computers and to certain situations where there would be Federal jurisdiction; in other words, two computers crossing State lines or a computer in one State and in a foreign country.

Good morning, Mr. Chairman; good to see you.

Senator LAXALT [presiding]. Good morning. How are you?

Ms. TOENSING. Fine.

Mr. Chairman, I was just praising you. You missed the praises on the record, but the Department of Justice was just thanking you and your staff and Senator Trible and his staff for all the work that you have put into this.

Senator LAXALT. Thank you.

Ms. TOENSING. It is looking good.

Senator LAXALT. Thank you.

Ms. TOENSING. We just have a couple more requests.

I was discussing the four principles that a computer crime bill should have. I just outlined two of them very briefly. The third one is covering computer destruction. We wanted it to be a crime to cover the destruction of any kind of Federal computer; and, fourth, a forfeiture provision.

If I could just go through those very, very briefly, Mr. Chairman, and tell you what little technical changes we would like to see.

On the computer access, the bill very ably covers unauthorized access if the computer is a Federal computer that is used exclusively by the Federal Government, but it does not cover it if it is a federally financed insured institution.

We think that they should be treated the same; that a person's financial records should not be accessed in an unauthorized manner any more than records in a Federal computer. What we would suggest is perhaps we could insert the word "observe" in the text, and my staff can work with—it is in my statement where it should be, but in addition to "obtain," to "observe," so that no one would be looking at someone else's financial records.

The second provision, the fraud provision, Mr. Chairman—the bill, as it is written, provides a fraud offense for Federal computers. We have two concerns with that. One of them is that it requires us to prove that not only is the computer accessed with the intent to defraud and that such access as furthered the fraud scheme and allowed the defendant to obtain something of value, but we also have to prove that this computer was accessed without authorization or that the person exceeded the scope of his or her authorization.

That concerns us. We are looking at the fraud offense as a fraud, and that is the heart of the crime; that is the sin that we are talking about. The unauthorized access is an additional sin that one should not do, but we would not like that as part of the fraud offense. Let me explain to you why on two counts.

One: What if the owner of the computer or Government supervisor is in on the scheme? It could make it difficult for us as prosecutors to prove that it was actually unauthorized because the person could have had permission to go beyond what we would consider to be the scope.

The other problem is it gets into a messy jury issue where you start arguing over whether the person was authorized or not authorized, and people forget to look at the real offense, which is the fraud or the scheme. Fraud is usually a very difficult element to prove in any event because frauds get very complicated when one has the mind to use a computer to commit a fraud.

The other point is that it does not track the old language that we know in our other fraud criminal statutes. The concern there, Mr. Chairman, is that when we walk into the courtroom and we talk about the language that we know in the fraud cases, we have a history. We have a precedential value in our fraud cases, so we know exactly what the courts are going to look at as to what constitutes a scheme to defraud.

This proposed bill has new language, and what the courts will do to us is they will say, "We know that the Congress knew what language was in the fraud statutes and now they have come up with

different language, so they must have meant a different kind of scheme or a different kind of standard."

If you feel that you may not want to put it in the statute, if in the report you could explain you meant the same kind of standard or scheme that we have always used in proving fraud cases, it would help us.

I hate to have another kind of fraud standard under the law for computer fraud. It does not make sense for us to have to prove different kinds of frauds for computers than we would have for someone committing a fraud otherwise.

Senator LAXALT. Well, does your proposed language track the existing language exactly or is it changed somewhat?

Ms. TOENSING. Your language does not track existing language.

Senator LAXALT. I know ours does not. But your proposed language, by way of modification, does?

Ms. TOENSING. Yes.

Senator LAXALT. Is that your intent?

Ms. TOENSING. Yes.

Just a minute, Mr. Chairman. I want to make sure—I know we submitted it at one time. It is in S. 1678, but my staff will be glad to work with anybody on your staff to show where to insert it.

Senator LAXALT. Well, your statement indicates you are tracking S. 1678. Is that true?

Ms. TOENSING. Yes.

Senator LAXALT. OK.

Ms. TOENSING. Two other just quick points, Mr. Chairman. On destruction, we would ask that you put into the $1,000 limit the amount of money that it would take to compute the lost computer time and the cost with redoing any program that could have been destroyed.

The last provision is forfeiture. Again, we feel that these are the kinds of cases where many times when people use computers, the courts, when it comes time for sentencing people, look at them as not going to be getting heavy sentences in this area.

So perhaps one of the deterrent angles would be to take away the thing that the computer criminal holds most dear, and that is the computer. We have proposed a forfeiture provision.

That is the extent of my remarks, Mr. Chairman. I would be glad to answer any questions.

Senator LAXALT. We thank you very much for your presentation. In addition, we thank you very much for the cooperation we have had from Justice in formulating this bill.

In connection with your proposed recommendations, I can say that, subject, of course, to the staff evaluation and eventual signoff, it appears that we can accommodate almost all your suggestions.

Ms. TOENSING. We appreciate that.

Senator LAXALT. We think they add materially to the bill. We have come a long way in this whole field. I know that I speak for the members of the subcommittee when I say that we had no idea until the hearings about the tremendous gap that we have in this whole field, and it is one that simply has to be covered.

Judging from what is happening on the House side and what we sense is happening here, it may well be that we will have some-

thing by the end of this year. I think it would be a remarkable achievement in the whole area.

So we thank you for your time and continued attention.

Ms. TORNSING. We thank you.

Senator LAXALT. Thank you.

[The prepared statement and responses to written questions follow:]

Department of Justice

STATEMENT

OF

VICTORIA TOENSING
DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

CONCERNING

S. 2281
THE COMPUTER FRAUD AND ABUSE ACT OF 1986

ON

APRIL 16, 1986

Mr. Chairman and Members of the Committee, I am pleased to be here today to present the views of the Department of Justice on S. 2281, The Computer Fraud and Abuse Act of 1986. As you know, I testified on October 30, 1985, before the Subcommittee on Criminal Law on the subject of computer crime and at that time discussed the shortcomings of the present computer crime statute, 18 U.S.C. 1030, and described the Administration's computer crime bill, S. 1678.

S. 2281 includes a series of amendments that would strengthen section 1030 of title 18; it also contains some provisions that are similar to those in S. 1678. Consequently, the Department of Justice supports S. 2281, although we will suggest some amendments which we think would further improve the bill. Let me first review some of the features we have said should be included in computer crime legislation.

First, there should be an offense proscribing the willful obtaining of unauthorized access to a computer owned by or operated or behalf of the United States or of a federally insured financial institution. This "trespassory" type of activity should be made a crime even without a showing that any information was obtained or that the unauthorized access prevented someone else from legitimately accessing the computer.

Second, there should be a computer fraud offense, patterned after the mail and wire fraud statutes, for fraud schemes involving computers with a particular federal nexus. We have suggested that the computer fraud offense should apply where the computer involved is owned by or operated on behalf of the United

States or a federally insured financial institution, or where the offense involves computers located in two or more states or in a state and a foreign country.

Third, it should be a federal crime to destroy willfully and without authority any computer owned by or operated on behalf of the United States or a federally insured financial institution, or any computer program or data contained in such a computer.

Fourth, computer crime legislation should contain a criminal forfeiture provision under which the defendant's interest in any computer involved in one of the three above offenses -- unauthorized computer access, computer fraud, or computer destruction -- could be forfeited to the government on his or her conviction.

Unauthorized Access to Computers

S. 2281, contains many of these provisions. First, subsection 2(b) of the bill amends present section 1030(a)(3) to make it an offense intentionally to make unauthorized access to a computer if the computer is used exclusively by the government of the United States. The amendment eliminates the requirement in the present subsection that the person who makes unauthorized access to a government computer must also use, modify, destroy, or disclose information in, or prevent authorized use of the computer. Thus, S. 2281 would establish a true unauthorized access offense for federal government computers. The offense would be punishable as a misdemeanor for a first offense, although a second conviction would be punishable as a felony. We

think this is the appropriate punishment level for this offense. 1/

By contrast, S. 2281 does not contain a "pure" unauthorized access offense for federally insured financial institutions' computers. Rather, it amends (in subsection 2(a) of the bill) subsection 1030(a)(2) to make it an offense to make unauthorized access to a computer and thereby obtain information contained in a "financial record" of a "financial institution." The

---

1/ The revision of subsection 1030(a)(3) would also cover unauthorized access to a computer used only part time by or for the government of the United States. The wording of this provision greatly alleviates another problem in the existing 1030(a)(3). Presently, 1030(a)(3) makes it a federal crime to make unauthorized access to and to use, modify, or destroy information in a computer "operated for or on behalf of the Government of the United States [if] such conduct affects such operartion." Grammatically, it would seem that this should require the government to prove only that the person's conduct affected the operation of the computer. However, the legislative history of this provision indicates that the prosecutor must prove that the unauthorized access to and the use or destruction of the information contained in the computer affects the operation of the government. See House Report No. 98-894, 98th Cong., 2d Sess., July 24, 1984, p. 22, for a discussion of the provision which became 1030(a)(3). It is our understanding that the revision of 1030(a)(3) in S. 2281 would make unauthorized access to a computer used part time by the government a federal crime if it could be shown that the unauthorized access was made at any time when the federal government was authorized to use it, or if the unauthorized "hacker" left some sort of message that was discovered when the federal government resumed its use of the computer. We would suggest, however, that to make this absolutely clear the revised 1030(a)(3) should read: "[Whoever] intentionally accesses a computer without authorization if such computer is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, if such computer is used by or for the Government of the United States and such conduct affects the use of the Federal Government's operation of the computer."

requirement that a person "obtain information" makes this something other that an unauthorized access offense. Since rummaging through bank files is, in our view, conduct deserving of punishment even if no information is actually obtained, and since federally insured financial institutions are deserving of the protection of federal criminal laws, we favor an unauthorized offense for this activity.

Nevertheless, subsection 3(a) of the bill, coupled with the bill's subsequent definition of "financial record" as "information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution," represents an improvement over the present subsection 1030(a)(2). The present 1030(a)(2) prohibits only unauthorized access to a financial institution's computer to obtain information in the account of an individual or a partnership of five or fewer persons. The revised 1030(a)(2) would reach obtaining information about corporate accounts at the financial institution, and loans to all individuals and business entities (since the individuals and businesses who have received the loans are all "customers" of the bank). 2/

2/ It would not, however, cover -- as we think should be covered -- obtaining information about the financial institution itself, such as its deposits in other banks, its loan policies and criteria, or lists of its shareholders.

Computer Fraud

S. 2281 also contains a computer fraud offense. Section 2(d) of the bill sets out a new subsection 1030(a)(4) which would punish one who "knowingly and with intent to defraud, accesses a Federal interest computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer." The term "Federal interest computer" is defined to mean a computer used by the United States Government or by a federally insured financial institution, 3/ or which is one of two or more computers used in committing the offense, not all of which are located in the same state. Thus, we think that the computer fraud offense in S. 2281 covers the type of computers in which there is a legitimate federal interest.

3/ The term "financial institution" is defined somewhat differently in S. 2281 from its definition in the Administration's bill, S. 1678. In both bills the term includes federally insured banks, savings and loan associations, and credit unions, and member banks of the Federal Reserve and of the home loan bank system. In S. 1678, the term also includes a member or business insured by the Securities Investor Protection Corporation and a broker-dealer registered with the Securities and Exchange Commission. These businesses are not included in the definition in S. 2281 although S. XXXX's definition does include any institution of the Farm Credit System under the Farm Credit Act of 1971." We are not opposed to covering Farm Credit System computers in the definition, but we believe computers of federally registered or insured brokerage firms are equally deserving of federal coverage.

However, the gravamen of the computer fraud offense in S. 2281 is misplaced, in our view. S. 2281 requires the government to prove not only that the computer was accessed with intent to defraud, and that the access furthered the fraud and allowed the defendant to obtain something of value (other than the use of the computer), 4/ but also that the access was without authorization or exceeded the scope of authorized access. 5/ As I said at the hearing last Fall, we can see no valid reason why a computer fraud offense should include a requirement that the government prove the defendant lacked authority, or exceeded his authority, to access the computer involved in the offense. What is involved is an economic crime, an attempt to steal money or other property. Whether it was done by authorized or

---

4/ S. 2281 does cover preventing authorized use of a Federal interest computer in a new subsection 1030(a)(5). That subsection sets out a felony of intentionally accessing such a computer without authorization and by means of one or more instances of such conduct altering information in the computer or preventing unauthorized use of the computer, if the person's conduct also causes a loss to another of $1,000 or more during any twelve-month period.

5/ S. 2281 substitutes the phrase "exceeds authorized access" for the cumbersome phrase "or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend" throughout section 1030. The phrase "exceeds authorized authority" is defined in a new subsection 1030(e)(6) as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled to so obtain or alter." We would suggest that this definition would be improved if the word "observe," was inserted before the word "obtain" both places it appears. This eliminates the problem of having to prove asportation, a difficult concept when an intangible, like information, is involved.

unauthorized computer access should be irrelevant. Proving the defendant's lack of authority could, in many cases, divert the jury's attention from what should be the central issue of whether the defendant devised a scheme to defraud, and if he did, did he access a computer in which there is some statutorily defined federal interest in carrying out the scheme. Again, we would urge the Committee to adopt this concept. Moreover, we recommend adoption of the computer fraud language contained in S. 1678 which tracks the mail and wire fraud provisions so as to preserve the considerable body of case law that has been developed under them, a familiar area of the law to the vast majority of federal prosecutors and judges.

Computer Destruction

For the offense of destroying a computer, a computer program, or computer data, S. 2281 sets out a new subsection 1030(a)(5) which is somewhat similar to the approach taken in S. 1678. The new 1030(a)(5) in S. 2281 would provide for punishment at the felony level for whoever "intentionally accesses a Federal interest computer without authorization, and by means of one or more instances of such conduct alters information in that computer, or prevents authorized use of that computer, and thereby causes loss to another of a value aggregating $1,000 or more during any one year period." It is our understanding that this is intended to be a "malicious damage" provision. The $1,000 threshold is intended to exclude such acts

as a hacker's leaving his name or a message on a covered computer, although I would note that if the computer involved was one owned by the federal government -- as opposed to a computer owned by a financial institution or one owned by a private party and accessed through another computer in another state -- such an act would still be punishable as a misdemeanor under 1030(a)(3), the unauthorized access offense.

The comparable offense in S. 1678 covers damaging, destroying, or attempting to damage or destroy a computer owned by or operated for the United States Government or a financial institution, or any computer program or data contained in such a computer. In drafting this provision, we felt that the role of the federal government should be limited, at least at first, to computer damage cases where the federal interest in the computer is the strongest. Accordingly, S. 1678 does not cover damage to a computer or computer data in one state by means of a computer in another state. If the Committee, nevertheless, believes that federal jurisdiction should be asserted over such an offense, at least where the damage amounts to $1,000 or more, we will not oppose it. We would, however, suggest that the legislative history of the proposed new subsection 1030(a)(5) in S. 2281 should make it clear that, in computing the amount of loss to reach the $1,000 threshold, such factors as lost computer time necessitated while erasing unauthorized entries in the computer, and the costs associated with checking and, if necessary, redoing an altered computer program should all count.

Forfeiture Provisions

S. 2281 does not contain a criminal forfeiture provision. As I indicated in my October testimony, forfeiture of the defendant's interest in the computer involved in the offense would often be an appropriate punishment, especially for a person convicted of the misdemeanor offense of making unauthorized access to a government computer. Realistically, few such persons are going to receive jail time for their first conviction. While they could receive a fine of up to $100,000, few defendants -- even the typically well educated ones clever enough to use their home or business computer to "hack" into a government computer network -- have anywhere near the type of assets necessary to pay such a fine. Forfeiture of the "hacker's" prized computer may be a very effective punishment, especially in cases where the defendant achieves a sort of "celebrity" status among his fellow computer buffs by having his defeat of the government's computer security system publicized by his misdemeanor conviction without any other real punishment.

Miscellaneous

In addition to those mentioned, S. 2281 makes other changes in section 1030 of title 18 which are generally helpful. It sets out a new offense in subsection 1030(a)(6) to proscribe trafficking in any password or similar information through which a computer may be accessed without information, with intent to

defraud, if the trafficking affects interstate or foreign commerce or the computer to which the password applies is used by or for the Government of the United States. It is our understanding that the conduct aimed at here is the creation and use of "pirate bulletin boards" used by "hackers" to display passwords to computers. Such an offense would appear to be warranted. Requiring that the trafficking be done with intent to defraud is too restrictive, however, with respect to the passwords for government computers. Selling or sharing at no cost passwords to allow a multitude of hackers to peruse government computer-stored information should be at least a misdemeanor, without any showing that the other hackers intended to defraud the government.

S. 2281 substitutes the word "intentionally" for the term "knowingly" in 1030(a)(2) and (3) for the mental state required for the offenses involving the unauthorized obtaining of information in financial institution computers and making unauthorized access to a Government computer. While we understand that this is intended as a slightly higher state of mind which would insure that an inadvertent computer trespass could not be prosecuted, we do not want it construed to prevent prosecution of a person whose initial access was inadvertent but who then deliberately maintained contact, perhaps for several days. In our view, such conduct should be prosecuted. We would prefer to retain the use of the word "knowingly" and allow the sound discretion of federal prosecutors to weed out the truly inadvertent (and quickly discontinued) computer trespasses. In the alternative, the

legislative history of the bill should include an averral of intent to reach the offender who "intentionally" maintains access after a non-intentional initial contact.

Mr. Chairman, although I have mentioned several areas in which we would prefer to see S. 2281 amended, it represents a substantial improvement over present law and over many other computer crime bills introduced in the Senate and the House. I would like to congratulate the Committee and its staff for its work in this difficult area. Mr. Chairman, that concludes my prepared testimony and I would be happy to answer any questions at this time.

DOJ-1986-04

U.S. Department of Justice

Office of Legislative and Intergovernmental Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

01 JUL 1986

Honorable Strom Thurmond
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

Enclosed are responses to questions submitted by you and by Senator Specter following the April 16, 1986, hearing on S. 2281, "The Computer Fraud and Abuse Act of 1986."

I hope this information will be of assistance to the Committee.

Sincerely,

John R. Bolton
Assistant Attorney General

RESPONSES TO QUESTIONS OF SENATOR THURMOND RE COMPUTER CRIME

Question 1: There are proposed amendments to Section 1030(a)(2) and 1030(a)(3). These amendments would replace the word "knowingly" with the word "intentionally" such that these aforementioned sections would require that prior to prosecution a person would have to "intentionally access a computer" as opposed to "knowingly access a computer." I believe that this requires a stricter standard of proof to successfully prosecute an act of computer fraud. Do you agree with my assessment of this amendment? Why or why not?

Response: S. 2281 would amend 18 U.S.C. 1030(a)(2) and (a)(3), sections which deal with unauthorized access to computers containing certain types of financial information and with unauthorized access to government computers, respectively. S. 2281 also adds a new computer fraud offense as 1030(a)(4). The state of mind for the new computer fraud offense is that the defendant acted "knowingly."

You are correct, however, in noting that the state of mind for the offenses set out in 18 U.S.C. 1030(a)(2) and 1030(a)(3) would be changed by S. 2281 from "knowingly" to "intentionally." This is a stricter standard of proof which, we understand, was added to insure that persons who inadvertently made the type of unauthorized computer access proscribed in these two provisions would not be prosecuted. As we noted in our prepared testimony, at pages 10-11, we would prefer to retain the use of the word "knowingly" and rely on sound prosecutorial discretion to weed

out truly inadvertent unauthorized access cases. Our concern here is that an "intentional" standard might be argued to preclude the prosecution of a person who inadvertently made an unauthorized access to one of the covered computers and then deliberately maintained contact for several days. We suggested that if the Committee decides to replace the word "knowingly" with "intentionally" in these provisions it make clear in the legislative history that it intends that the revised provisions are still intended to reach a person who "intentionally" maintains access after a non-intentional initial contac..

Question 2: This amendment creates new offenses. One such offense allows for prosecution of an individual who after accessing a computer alters information in that computer. (1) What particular problems have there been with individuals who access a computer and then alter information? (2) Once this information is altered or destroyed, is it possible to replace it?

Response: There were at least three instances in 1985 where, for a fee, persons used their home computers to alter other persons' credit ratings in credit reporting agency files. The operator of the computer simply views and alters, but does not "obtain" the credit history information as is required under 18 U.S.C. 1030(a)(2) as it is presently written.

There are, of course, a wide range of other institutions not covered by the statute such as motor vehicle departments, universities, hospitals, and insurance companies where the same thing could happen. Simply changing an address in a computer file for the delivery of funds or sensitive equipment and then changing the file back so that it reflects the proper address is another type of problem.

If the organization whose computer is involved has "backed-up" the altered file and stored the back-up separately, the information could be restored. Otherwise, altered information typically stays altered.

Question 3: Are the majority of the problems with illegal computer access centered around inside employees or outside individuals?

Response: It has been our experience that most illegal computer access problems are centered around inside employees. We base this primarily on the fact that the majority of the approximately 50 computer related cases investigated by the agency Inspectors General in the past three years have been employee-related. Outside access is a recent phenomenon due to improved technology.

RESPONSES TO QUESTIONS FROM SENATOR SPECTER RE COMPUTER CRIME

Question 1: Although the Comprehensive Crime Control Act of 1984 addressed computer-related offenses, new legislation may be needed in this complex area. What is your view regarding the inclusion of new offenses for theft or intentional destruction of computer data?

Response: We think both offenses should be included as part of any computer crime bill. Both are in S. 2281.

Question 2: This legislation being considered today presents a different approach to new, complex crimes involving the use of computers. What is your view regarding the bill's distinction between theft of information and unauthorized access? Do you believe the penalties in the legislation are adequate for this felony and misdemeanor respectively?

Response: S. 2281 would amend 18 U.S.C. 1030(a)(3) to proscribe making unauthorized access to a computer used exclusively by the Government of the United States or to a computer used part time by the government if the unauthorized

access affects the government's use. In a prosecution under the revised section 1030(a)(3) it would not be necessary for the government to prove that the defendant obtained anything of value, such as information. For that matter, it would not be necessary to prove that the defendant even observed any particular information or data in the computer system, just that he made the access without authority.

S. 2281 would also amend 18 U.S.C. 1030 by adding a new paragraph 1030(a)(4) setting out a computer fraud offense. It would proscribe accessing a "Federal interest computer" (a term defined in the bill) without authority or in excess of one's authority, knowingly and with intent to defraud, and by means of such conduct furthering the intended fraud or obtaining anything of value other than just the use of the computer. Clearly, the phrase "anything of value" would include information contained in the computer. One who obtains information obtains much more than just the use of the computer. Merely obtaining the use of the computer (without the additional showing that some information was obtained) is to be punished as an unauthorized computer access.

We have no objection to this distinction between theft of information in a computer and unauthorized computer access. We also believe S. 2281 strikes the proper balance in punishing the "obtaining information" offense as a felony and the unauthorized access offense as a misdemeanor. We note that a second conviction of the unauthorized access offense would be punished as a felony. We also favor this provision.

Question 3: The complexities of computer-related crime raise specific issues as to defining jurisdiction. What is your view regarding the bill's limitation of Federal jurisdiction to felonies? Do you believe setting a specific loss value pursuant to the legislation is a viable means to define jurisdiction? Do you have any additional suggestions regarding the jurisdiction issue?

Response: Initially, as indicated in answer to the last question, federal jurisdiction is not limited to felonies. There is federal jurisdiction over the misdemeanor of making unauthorized access to a computer used by the United States government. I might add that a new federal offense of trafficking in computer access passwords, set out as a new 18 U.S.C. 1030(a)(6), is also made a misdemeanor.

S. 2281 does, however, set out a specific loss value in its creation of a computer damage offense, the new 18 U.S.C. 1030(a)(5). This offense punishes as a felony the intentional accessing of a federal interest computer and either altering information in the computer or preventing authorized access to the computer, thereby causing a loss of $1,000 or more during a one year period. The setting of the $1,000 floor was apparently an attempt to ensure that only cases involving a significant loss were prosecuted as federal felonies, although as we explained at page eight of our prepared statement if the computer involved was one owned by or operated on behalf of the federal government, the offense could be punished as a misdemeanor under 18 U.S.C. 1030(a)(3), the unauthorized access offense. Normally, the Department of Justice opposes provisions requiring the proof of a specific loss value because they can provide difficult problems of proof and lead to unjustifiable acquittals of guilty defendants. Nevertheless, we realize that substantial support has developed for this provision, and have not opposed it. However, in our prepared statement we suggested that the legislative history should make it clear that a number of factors should be counted in reaching the $1,000 floor such as lost computer time while erasing unauthorized computer entries and the costs associated with checking and, if necessary, redesigning an altered computer program.

Senator LAXALT. Our next witness, then, will be Joseph Tompkins, who is an attorney here with Sidley & Austin.

Mr. Tompkins, we thank you for your past cooperation and help through the ABA. It is my understanding that you do not have any written statement, as such, and that is probably refreshing.

STATEMENT OF JOSEPH TOMPKINS, ATTORNEY, SIDLEY & AUSTIN, WASHINGTON, DC

Mr. TOMPKINS. I apologize for not having a written statement, Mr. Chairman. It was only a few days ago that I was asked to present testimony, but I will be glad to submit a written statement following the hearing today if that would be helpful.

Senator LAXALT. That would be entirely satisfactory.

Mr. TOMPKINS. Thank you.

Senator LAXALT. I would like you, for the benefit of the members of the committee, to give us your frank impressions of the present legislation together with some of the modifications that have been proposed by Justice and others.

Mr. TOMPKINS. I will do the best that I can.

As I think you know and others know, I have been serving as chairman of the ABA Criminal Justice Section Task Force on Computer Crime, and it is our task force that published the computer crime report in June 1984.

For that reason, we have kept close track of the legislation on the subject.

Senator LAXALT. Incidentally, for the record, the report has been enormously helpful to us in the process of this legislation. We thank you for that.

Mr. TOMPKINS. Well, I appreciate your saying that. The response to the report has been—I think overwhelming would be an accurate description of the interest and the followup that we have had after it was published.

I should make clear that any remarks I make today are my views only. I am not in a position to speak on behalf of the ABA.

Senator LAXALT. The record will note the disclaimer.

Mr. TOMPKINS. Or for anyone else, for that matter.

In general, I think the proposed revisions included in the legislation are a step in the right direction. They broaden the scope of the existing computer crime statute in some laudatory ways.

They clarify some terms and provisions of the existing statute in a useful way, and they refine and rationalize some of the sanctions available.

Senator LAXALT. Have you had to work with the bill yourself as a practitioner?

Mr. TOMPKINS. I have given advice to some clients on the bill, yes, sir. I have not been involved in a proceeding under the bill.

Senator LAXALT. In terms of working with the bill within the courts, have there been problems in connection with terminology, vagueness, and that sort of thing?

Mr. TOMPKINS. I can only speak secondhand. I have talked to prosecutors who have tried to use the bill, and I know in a previous hearing this past fall an assistant U.S. attorney here in the District

who was doing a grand jury investigation trying to use the statute indicated he had some problems, and he identified several.

One was with the so-called use exemption, which is part of section (a)(3). The proposed legislation would eliminate the use exemption, and I think that is one of the clarifying points that is useful.

However, it still has a phrase "affects such use," and one suggestion I have is, the committee may consider defining what "affects such use" means, what that phrase means.

There also have been press reports of other prosecutors. I know one in Denver who was faced with a constitutional challenge when she was trying to prosecute somebody under the existing statute, and the defense was asserting that it was unconstitutionally vague.

I do not know whether that ever went anywhere, but there have been——

Senator LAXALT. What did the trial court do with it?

Mr. TOMPKINS. I have not heard the outcome.

Senator LAXALT. OK.

Mr. TOMPKINS. But that was a problem that was raised.

Perhaps I could get to some specific comments about the proposed bill, and I will focus on the new provisions that are being proposed to be added.

The existing provisions sections (a)(1), (a)(2), and (a)(3) are amended-ed in some form by the proposed legislation, and I think the amendments are helpful. They use the phrase "exceeding authorized access" instead of the other cumbersome phrase, and it defines what that means, which I think is helpful.

Section (a)(2) is also being broadened by including a broader definition of "financial institution," and I think that is commendable as well. I would note that section (a)(2) still does not cover certain financial records. Specifically, it would not cover corporate financial records of a confidential nature that are not stored within one of the institutions that is within the definition of "financial institution."

These records, similar to individuals' credit records, are stored in the equivalent of corporate credit agencies, such as Dun and Bradstreet, Moody's, and other entities. I have, just through conversations, discovered that there have been problems with people intruding in confidential corporate records which are kept in these kinds of agencies.

That would not be covered by the legislation. I think that is something the committee may want to consider as a further broadening of the act.

Senator LAXALT. Do you see any downside to that?

Mr. TOMPKINS. The downside would perhaps be, if it was too broad, it would maybe give some zealous prosecutors too much authority or it would open the door to perhaps more litigation than the committee intends.

The other argument is that people can protect themselves and why cannot the corporations civilly go after people that intrude on their records. I think that is a partial answer, but I am not sure that that should be exempted from criminal sanction.

Senator LAXALT. Give us some suggested language.

Mr. TOMPKINS. I will be glad to do that if I have a little more time to come up with something.

Senator LAXALT. You can do it on your own. We will not tie it to the ABA or anybody else.

Mr. TOMPKINS. All right.

Section (a)(3), I think, is improved for the reasons I mentioned, getting rid of the use exemption. That is where the phrase "affects such use" occurs, and my suggestion would be, to avoid perhaps unnecessary and costly litigation over what that phrase means, the committee may want to define what "affects such use" means.

In a number of State computer crime statutes, "use" is normally defined, and "affects such use," if that phrase is used, has been defined.

Let me get to section (a)(4). That is the——.

Senator LAXALT. Justice, incidentally, has made that same recommendation.

Mr. TOMPKINS. I concur with that.

Section (a)(4) is the new fraud provision. I agree with some of the comments that Ms. Toensing had about that Specifically, I agree that the committee should consider, if not exactly tracking the language of the wire and mail fraud statutes, perhaps modifying the language to make it similar to that.

A second comment on that—the proposed provision would seem to require premeditation; that is, the intent to defraud would have to be formed before someone accessed improperly a computer.

There have been instances that we know of where someone improperly accesses a computer, not knowing what they are going to find. They find credit card records or other financial information, and at that point they decide they are going to use that to defraud someone.

Senator LAXALT. Could not the intent be formed at that point?

Mr. TOMPKINS. It would be. The wording of the statute would seem to say that at the time of the access there has to be an intent to defraud.

Senator LAXALT. And the intent could not be formed later even though the original access was innocent?

Mr. TOMPKINS. Technically, a literal reading of the statute would seem to say that that is not covered if the intent was formed later. A wording change to say whether the intent was formed before or after—I mean, again, that is an easy modification to make.

Senator LAXALT. I think you are probably right. If you read it technically, the intent to defraud really is tied and linked pretty closely, if not totally, to the original access.

Mr. TOMPKINS. That is my reading of it as well.

Senator LAXALT. All right.

Mr. TOMPKINS. Section (a)(5) is the provision I would like to focus on the most. There are a number of comments I have on that. One is, the provision covers the alteration of information. I am not sure whether it would cover the destruction of information or data.

Arguably, "alter" would include "destroy." Most of the State statutes on the subject include the words "alter or destroy," and I would suggest that be added before "information."

Also, my reading of the provision is that it would not cover the destruction or alteration of computer software. Software is normally treated differently than the data itself which is in a computer.

"Information" normally means the data and not the program, not the software that runs it.

That particular kind of computer crime is one that we identified in our report. It was one of the most frequently mentioned types of computer crime that affected the people that responded to the survey.

Senator LAXALT. I am glad you raised that because it has never been the intent of any of us to exclude software. You think we need language, then. Is that what you are saying?

Mr. TOMPKINS. Well, my suggestion would be that the phrase—it could read "alter or destroy information or computer software"; that those words be added to make it clear that that is covered by the legislation.

If you do that, then you probably need to define what you mean by "computer software," and there are a number of State statutes that define that as well.

Senator LAXALT. Is there a rather common definition on the State level as to what constitutes "software"?

Mr. TOMPKINS. I think the definitions are similar and it is being used enough now in litigation that coming up with a generally-accepted definition should not be that difficult.

Then later in the provision, it speaks of altering information in that computer, thereby causing loss to another of a value aggregating $1,000 or more during any 1-year period.

The question that occurs to me is what about the accessing of multiple computers to cause a loss aggregating more than $1,000. In other words, the way the statute reads, it is specific to "that computer" that was accessed.

In a number of cases, someone will do the same scheme, access a number of computers, and maybe not cause a loss over $1,000 in each computer. But if you add up the losses they incur, they are over $1,000.

So my suggestion would be to say "in such a computer" instead of "in that computer" to cover the multiple——

Senator LAXALT. Do you think that would do it?

Mr. TOMPKINS. Well, given the few days I have had to think about it, that is what occurred to me.

Senator LAXALT. Well, tell me again now. You would insert it where? "Or prevents authorized use of that computer"—you would include it there?

Mr. TOMPKINS. Instead of the phrase "in that computer," it should read "in such a computer."

Senator LAXALT. Oh, I see, and you would add what, now? How would you change the phrase "in that computer?"

Mr. TOMPKINS. With the changes I have talked about before, it would read "such conduct alters or destroys information or computer software in such a computer."

Senator LAXALT. "In such a computer."

Mr. TOMPKINS. Somebody else with a sharper eye may come up with a better phrase than that.

Senator LAXALT. Yes, all right. We see where you are going.

Mr. TOMPKINS. That is the point, anyway.

Senator LAXALT. OK.

Mr. TOMPKINS. There is also the question of what about a person who accesses a computer and obtains information which allows him or her to impose small losses on hundreds or thousands of people.

The way this is worded, it talks in terms of a loss "to another" and arguably would not include the cases that we know about where someone gets in a computer, gets the records of many individuals, and causes perhaps $50 in losses to 10,000 people.

The argument could be made that this does not cover that.

Senator LAXALT. Do you think the fraud provisions might?

Mr. TOMPKINS. The fraud provisions might, and specifically if it were credit card fraud, I think section 1029 would probably cover that. What I am thinking of is there are people who are able to access computers and destroy similar kinds of software where the individual would lose a $50 software program or a $100 software program, and do that to a lot of people.

To avoid the argument that that is not covered by this because each individual that is affected has to incur a loss of $1,000, that is the point that I am raising.

Senator LAXALT. All right.

Mr. TOMPKINS. My suggestion would be to make it read "thereby causes losses to one or more persons aggregating $1,000 or more during any 1-year period." And then you might want to consider defining "person" to include individuals, institutions or Government agencies to make clear what that phrase means.

The committee might also want to consider defining what loss encompasses, because that is another phrase that can be ambiguous and State statutes normally define it.

Another issue that you might want to consider is there may be instances in which the perpetrator improperly gains something of value but causes no direct loss to another person.

For example, if a competitor gains access to the computer records of a firm's actual or potential customers or marketing plans, that firm may be able to gain substantial income from it, but it may be difficult to prove a direct loss to the company that was the victim.

Again, in a situation like that, perhaps there could be civil recovery by the victim, but I raise the question of should that conduct where the perpetrator gains a lot but there is no provable, direct loss to the victim—should that be covered as well in a criminal statute? I just raise that as a question.

Regarding the $1,000 or more loss requirement, as I read the analysis that accompanies the bill, the explanation is that that is not a jurisdictional amount. In other words, that is a felony and a misdemeanor-determining factor and if you do not meet the $1,000, then you get kicked back to (a)(3), which is the trespass statute.

As I looked at it, it became apparent to me that the coverage of (a)(5) is not the same as the coverage of (a)(3). In other words, they are not coterminous. Specifically, (a)(5) covers so-called Federal-interest computers, and those are defined to mean computers exclusively for the use of a financial institution or the U.S. Government, or which is one of two or more computers used in committing the offense not all of which are located in the same State.

Now, if you do not get in under (a)(5) because of the $1,000 limit and you get, therefore, put back to (a)(3), (a)(3) applies only to computers used exclusively by the U.S. Government, or if not exclu-

sively used, it is used to some extent by the Government and the conduct affects such use.

I guess the point is it is not really a felony-misdemeanor cutoff. It is, in a sense, a jurisdictional cutoff because if you do not make it under (a)(5), there are instances—for example, if one improperly accesses a nongovernment computer across State lines and a $1,000 loss to another cannot be shown, then in that instance you do not fit within either (a)(5) or (a)(3).

Senator LAXALT. That is correct, apparently.

Mr. TOMPKINS. That is a gap that I think you might want to plug. I guess the question might be, if you cannot show a $1,000 loss, why should we be concerned? I think some of the discussion that the Department has made about the $1,000 loss and the difficulty of proving that applies.

But there have also been instances, and the Sloan-Kettering Cancer Institute is an instance, where there was the infiltration of hospital records and the alteration of those records, and that occurred across State lines.

You cannot show a $1,000 loss from that directly, but you can show that some patients may have been harmed. That is the kind of thing that, to me, should be covered. Under the proposal, it would not be.

One way to fix it would be to eliminate the dollar threshold and make punishment dependent upon the loss incurred or the value obtained, with flexible definitions of each. I think that was the approach used in some of the earlier legislation.

Another way to do it would be to make (a)(5) and (a)(3) coterminous in terms of their scope.

The final point I would make, and I apologize for going on this long, is really a problem and I raise it as something that I do not have a clear answer on how it should be dealt with, but maybe it could be dealt with in the legislation. That is the so-called Trojan horse problem.

As you probably know, there are computer programs which are designed essentially to destroy other computer programs. One particularly devious scheme which has been used with some frequency is to entice computer owners to accept these program-devouring programs without knowing what they are.

This is often done by advertising these Trojan horse things on electronic bulletin boards, describing them as program enhancements. Once the invitation is accepted, the unsuspecting computer owner finds that instead of enhancing his program, what he has gotten off the bulletin board has destroyed his program.

The problem, of course, is that those losses are, in a way, self-inflicted. If the person had not tried to get the program off the bulletin board, he would not have incurred a loss.

But they are really the result of a trap that has been set for the unwary by shrewd and evilminded perpetrators. Those schemes are not covered by the existing law and they would not be covered by the proposed legislation

Designing language to encompass those without being too broad is a challenge for all of us. I do not have any specific language, but I raise that for you and the members of the committee as something to be considered.

I would just conclude by saying that there are additional suggestions that could be made in terms of additional definitions—words such as "access" or "authorization" that could be defined to make the statute a little more clear.

Something that I testified about a couple of times before House subcommittees is the addition of civil remedies to a law such as this. That has been done in several States, including Virginia, and there are arguments on both sides of doing that.

Senator LAXALT. Has it been helpful?

Mr. TOMPKINS. I think the experience in Virginia has been that it has been helpful. Given the scarcity of law enforcement resources, often it provides a means for a civil victim to deal with the problem so that law enforcement does not have to get involved.

The downside of it is, it creates a civil remedy and it adds to the litigation and the burdens on the courts.

Senator LAXALT. Is there no common law remedy?

Mr. TOMPKINS. There can be, I think, in some instances, but it is not always clear that there is. The common law was not developed at a time when computer programs were in operation, so that creates a difficulty.

So the civil remedies thing I would raise again as something to be considered. The final point is the issue of concurrent jurisdiction and the issuance of guidelines for the exercise of Federal jurisdiction.

I know that is something that has been dealt with in some of the previous legislative proposals, either putting the guidelines in the legislation or requiring the Attorney General to develop those.

I think that is worthy of consideration, and I know some of my colleagues in the ABA who are State and local prosecutors are very concerned about that.

So, with those comments, I thank you for the privilege of being here, and I commend the committee on the work it has done.

Senator LAXALT. Well, we thank you, Mr. Tompkins. Once again, you have been very helpful. I do not know whether there will be a need for you to submit anything. We have a record here. If you have some additional suggestions, pass them on, and there will be some time here before we go to the full committee markup.

We thank you very much again for your time and attention and help.

Mr. TOMPKINS. I may be able to do it better in writing than I can orally.

Senator LAXALT. You do very well orally.

Mr. TOMPKINS. Thank you.

Senator LAXALT. Thank you.

Very well. Our next witness is Mr. John Sponski, who is group executive officer at Sovran. Mr. Sponski is also representing the views of the Virginia Bankers Association. He testified at the subcommittee hearing that I chaired last year.

You, also, Mr. Sponski, have been enormously helpful to us in the formulation of this legislation and particularly these modifications.

Mr. SPONSKI. Well, thank you, Mr. Chairman.

Senator LAXALT. Proceed in any manner that you wish.

STATEMENT OF JOHN J. SPONSKI, GROUP EXECUTIVE OFFICER, SOVRAN FINANCIAL CORP., RICHMOND, VA

Mr. SPONSKI. In view of the fact that I did testify before you last year and you graciously heard my written statement at that time, why do we not just insert that into the record, and what I would like to do is just cover some summary points of my comments.

First of all, I want to point out that the Virginia Bankers Association and Sovran Financial Corp. want to encourage you and your committee to speedily pass this legislation.

The importance to our business of computer systems and our data bases cannot be sufficiently stated. We have recognized this, and for years we have spent considerable funds and taken extensive measures to attempt to restrict access to our systems.

But, very frankly, every time we put in a safeguarding measure, people who have intentions of intruding into your system, who are quite intelligent and very sophisticated, will find some way to get around it.

This is so vital to our business that our concern is the confidence of our customers and the privacy of their financial information—that their confidence in us as institutions and protectors of that private information is being eroded, not necessarily because specific incidents have occurred, but because so much is being written nowadays about the skill of backers and their opportunity to get into systems.

It is absolutely vital that we have effective, simple legislation as soon as possible.

Now, this morning I have heard a couple of things that I want to talk about for a moment. I have heard this phrase called "accidental access." Frankly, in my mind, there is no such thing as accidental access into a computer system or into a data base.

One could randomly generate a telephone number and accidentally get into a computer system. But with the safeguards in effect at that time, you would have to take a deliberate measure to attempt to develop what the access code is to allow you to come into that computer system.

Let us say even if you did that accidentally and by some quirk your normal access code happened to be also an authorized access code in that particular system, that computer system would then identify itself to you and you would surely know at that particular point that it was not what you were trying to get into.

If you continue at that particular point, then in my mind you are doing it deliberately and not as a case of accident.

Senator LAXALT. Good point.

Mr. SPONSKI. So the statistical probability of an accidental occurrence happening without the intruder being aware of it as an unconscionable act is just nonexistent.

The second point is casual perusal. I have heard a lot of comments today both from the Justice Department and the representative from the ABA talking about if you are into the computer system, but you do not do any damage to it, or changes less than $50, et cetera.

Casual perusal does as much to jeopardize the confidence of customers and our ability to provide and protect the information that

they have entrusted to us. Now, what I mean specifically by casual perusal is that someone gets into a system and then literally goes in and says, let's see what is in it; let me find out the information about, for example, the chairman of our bank—what is he depositing in his account, what type of accounts does he have, et cetera.

Now, in that case, there has been no transfer of funds; there has been no alteration whatsoever of software code or data that is in the file. But the intruder is, in fact, using a data base for purposes for which it was not intended. He is not an authorized user.

I think that casual perusal should be treated with as much severity as going in and deliberately changing codes or altering financial records.

The last part that we wanted to bring to your attention, and we certainly appreciate that the committee is attempting to be responsive to meeting this threat to our privacy considerations for our customers, is that the penalties, I think, have to be significant.

You recall in October when I testified before you at the time, I used the analogy that today, because of legislation that occurred in the 1930's, when one robs a bank, it is not a casual occurrence. One recognizes that you are taking a very large step when you go and rob a bank because Federal legislation immediately requires that Federal investigative agencies come into play whenever a bank has been robbed.

Today, looking at the proposed penalties in the bill, I am concerned if it will really detract the intruders and the hackers from coming into the systems. Is there enough teeth in the penalties to make the intruder understand that if I am going to play this gambit, in fact, it becomes a serious offense and very technically capable Federal investigative agencies will come into play in this?

It is not going to be that somebody in the sheriff's department may have this on a part-time basis, or some member of a local police department. In fact, the power and the experience and expertise of a Federal investigative agency such as the FBI or the Secret Service is going to come into play, and this becomes very serious business.

So I think that what we are looking for is we recognize the Federal legislation today which has been in effect for many years has not prevented bank robberies by any case, but it certainly has made it a very serious offense and I think has discouraged people from casually going in and robbing an institution, recognizing the implications of that step.

We think the same thing needs to be applied in the case of these intruders and hackers coming into data bases; that that is a very serious intrusion into the system.

That is all I wanted to bring to your attention, Senator, and we do appreciate that you and your committee are attempting to get this legislation passed as quickly as you can.

If there is any question I can help you with, with my background in data processing as well as bank operations, I would be glad to help you or your committee on it.

Senator LAXALT. Well, we appreciate that greatly. Again, we thank you for coming in this morning and offering, as you have in the past, some constructive suggestions. We will stay in touch.

Mr. SPONSKI. Thank you, Senator.

[The prepared statement follows:]

TESTIMONY BEFORE
THE COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

BY

JOHN J. SPONSKI
GROUP EXECUTIVE OFFICER
SOVRAN FINANCIAL CORPORATION

Mr. Chairman and Members of the Committee:

My name is John J. Sponski. I am a Group Executive Officer within Sovran Financial Corporation with responsibility for Operations and Data Processing in Sovran Bank, N.A. Sovran Financial Corporation headquartered in Norfolk, Virginia, is a multi state Financial Institution with banks in Virginia, Maryland, and the District of Columbia. As of December 31, 1985, Sovran Financial Corporation had assets of $13.0 billion. Sovran Financial Corporation provides commercial banking and related financial services and products to its customers through a network of 357 branches and 297 automated teller machines in over 150 communities in VA, MD, and DC. Sovran Bank, N.A. in Virginia is a member of the Federal Reserve System; and its deposits, which totaled $7.2 Billion as of December 31, 1985, are insured by the Federal Deposit Insurance Corporation.

This morning I represent not only Sovran Financial Corporation, but also the 168 member banks of the Virginia Bankers Association. We strongly support and recommend passage of legislation to discourage and deter unauthorized access to and use of computer systems maintained by Financial Institutions. Although some states currently have statutes which provide for fines or imprisonment for those residing in the state, who access and use financial institution computer systems without authorization, these measures are inadequate since they do not address incursions into systems originated by intruders outside a state through use of current telecommunications technology.

Sovran Financial Corporation strongly supports Federal legislation to combat the risks of exposure to loss from unauthorized incursions into our computer systems by an increasing number of people who have the knowledge of and access to technology. Simple, and effective legislation is needed, now, to discourage and punish unauthorized incursions, particularly, when initiated outside a state's boundaries.

I am confident that the members of this Committee appreciate the importance to the Financial Industry of computers and information data bases. Most products and services provided by Financial Institutions could not be provided without computers and information data bases. Today, many within the Financial Industry consider our basic function to be information transfer to our customers rather than just depository/lending services.

Through the information stored in our data bases we are able to provide customers with timely, reliable information on their financial condition, so they can transfer funds with confidence and invest wisely.

Currently, the value to a Financial Institution of the information stored in its data bases far exceeds the value of its vault cash. In many ways information is more valuable than cash because of its potential for use. Through our information data bases we meet our customer's financial service needs; analyze data for marketing strategies and programs; provide various reports to regulatory and governmental agencies; and, of course, maintain our own corporate records. Financial institutions today cannot function without timely, accurate and detailed information data bases.

Sovran Financial Corporation's use of and reliance on computers reflects a prevalent condition in the Financial Industry. The Sovran Financial Corporation currently has 10,515 employees. We have over 6,000 terminals connected to our computers. These terminals are used by our employees and our customers. Daily, over 800,000 transactions or requests for information are entered through these terminals. At present, Sovran has 172.8 Billion Bytes of data stored on our disk units. If we were to print out this data on computer paper with 7,500 characters per page,

this would result in a report 3,271 miles long, the distance from San Diego, California to Acadia, Maine. The information we have on our computer systems is proprietary in the sense that it is ours, obtained from our customers to meet their financial service needs. This information is also private since it is about our customers and that most confidential subject - their money. In this regard, the information has been entrusted to us.

Recognizing our responsibility to safeguard this valuable asset - information, Sovran Financial Corporation and other institutions have in use various means to control access to our information data bases. At Sovran we employ a series of progressively restrictive access control methods. These measures include restricting access to data bases to only those employees who must use the information to service customers; requiring unique access codes assigned to each terminal user to identify and monitor entry to the data bases; requiring quarterly changing of access codes; protecting application systems with highly structured terminal control systems which limit use of terminals to specific individuals, by function, by type of transactions and other criteria; by employing dial-back techniques for systems accessible to dial-up terminals; and lastly, selective use of message authentication or encryption of data. These are elaborate and expensive measures we have taken to protect this valuable asset - information. But the true value in information is its use and, consequently, control systems, no matter how effective, must permit access to the information for use.

The most effective way to protect anything of value is to put it into a vault constructed of thick reinforced walls with elaborate sensitive alarms. To provide absolute security this vault does not have a door - so the valuables cannot be removed. This is absolute security. Information stored in a data base in such a way as our vault is indeed secure. But it is also frankly useless and valueless since it could not be accessed for use.

Sovran Financial Corporation and other Financial Institutions have installed reasonably effective and practical safeguards

for their Information Data Base. However, the rapid advances of technology, the extensive development of telecommunications systems, and the ready availability of powerful microprocessors, matched with the increasing knowledge and experience of many within our nation about computer systems are eroding our safeguards. Computer 'Hacking' is an intellectual challenge for many. For those so inclined it has replaced the intricate strategies and thought processes of a chess game. This interest in 'Beating' an institution's access control system will not diminish so long as intruders receive notoriety in the media and verbal reprimands from authorities cautioning them to put their talents to other applications.

In 1984, the Computer Crime Task Force of the American Bar Association surveyed 1,000 private organizations concerning the nature and occurrence of computer related crime. Seventy-nine percent of the respondents indicated support for a Federal criminal statute as needed to combat unauthorized intrusions into computer systems. Sovran Financial Corporation and the 168 member institutions of Virginia Bankers Association are also strongly in support of a federal statute which would deal with computer intrusions occurring, both intra and interstate. Intruders are not limited by state boundaries. Low cost long distance systems permit an intruder to make their gambit at a most reasonable cost.

A Federal statute imposing imprisonment terms of consequence will complement the efforts taken to date and planned by Sovran Financial Corporation and other Financial institutions to protect and restrict access to data. But since use compels us to add a door to our perfect vault, so also must we provide a door to our information systems. Just as it is a violation of a Federal statute to rob the vault of a Bank, we believe it should also be a violation of a Federal statute to gain entry without authorization to an information data base; or to misuse an information data base when access is authorized; and most certainly when data is altered, added, or deleted within an information data base without authorization.

Without a Federal statute to discourage unauthorized entry into information data bases, any measures or technique will, as in chess, be countered by a skillful, talented and highly intelligent Intruder or Hacker. Of course, existing Federal statutes have not eliminated bank robberies. But these statutes have definitely discouraged a casual attitude toward robbing a bank. A Federal statute which requires the intervention of Federal Investigative Agencies into incidents of unauthorized access to and misuse of information data files will not eliminate every occurrence but it will certainly increase the penalties of the game.

Mr. Chairman and members of the Committee, we know you must consider and evaluate many requested Federal statutes; but we earnestly request you to act speedily to pass legislation to provide an additional measurement of protection to the vital information data bases and computer systems, both in existence and under development, in our progressively technologically dependent nation.

Thank you for this opportunity to present the concerns and recommendations of Sovran Financial Corporation and the Virginia Bankers Association.

Senator LAXALT. I would like before we close the record to, if there is no objection—I do not see any—file a statement by Senator Denton for the purposes of the record.

[The following was received for the record:]

PREPARED STATEMENT OF SENATOR JEREMIAH DENTON

Mr. Chairman, I strongly support and am proud to be an original cosponsor of S. 2281, the Computer Fraud and Abuse Act of 1986. I congratulate and commend my distinguished colleague from Virginia, Senator Trible, for introducing this important legislation, and I thank the chair for its leadership in expediting committee consideration of the bill.

The rapid evolution of computer technology has required us on several occasions to reassess the adequacy of our existing criminal statutes to deal with the novel patterns of criminal activity made possible by the widespread use of computers. For instance, in June 1985, as chairman of the Senate Judiciary Subcommittee on Security and Terriorism, I chaired a hearing on the use of computers to transmit material that incites crime and constitutes interstate transmission of implicitly obscene matter. That hearing yielded abundant evidence of various courses of criminal conduct which were difficult or impossible to prosecute under existing law because the conduct occurs, in whole or in part, through computer transmissions.

The bill which is the subject of today's hearing, S. 2281, is intended to deal with crimes spawned by the "Computer Age." The bill clarifies and strengthens existing Federal protections against computer crime and creates new offenses to deal with cert. in acts which are not now crimes under Federal law, such as theft by computer with the intent to defraud and the intentional destruction of computer property, when those offenses are committed on an interstate basis or involve the computers of federally insured financial institutions.

S. 2281 addresses computer crimes which are properly matters of Federal concern. The legislation is needed to keep our criminal code relevant to such criminal activities, which are made possible by the continually developing technology in the computer field. I urge my colleages on the Judiciary Committee to report the bill favorably to the full Senate.

Thank you, Mr. Chairman.

Senator LAXALT. Very well. We will stand adjourned. Thank you all.

[Whereupon, at 10:41 a.m., the committee was adjourned.]

O

62-543 (56)